

AP/2143
IFW

ATTORNEY DOCKET NO. BLEICHENBACHER 4-27

PATENT



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Daniel Bleichenbacher, *et al.*

Serial No.: 09/625,817
Filed: July 26, 2000
For: SYSTEM AND METHOD FOR EXACTING A
SYSTEM RESOURCE ACCESS COST
Grp./A.U.: 2143
Examiner: Mitra Kianersi

CERTIFICATE OF FIRST CLASS MAILING

I hereby certify that this correspondence, including the attachments listed, is being deposited as First Class Mail with the United States Postal Service, in an envelope addressed to Commissioner for Patents, Alexandria, VA 22313, on the date shown below.

08/05/2004
Date of Mailing

Stephanie Pratt
Signature of person mailing

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Mail Stop Appeal Brief-Patents

ATTENTION: Board of Patent Appeals and Interferences

Sirs:

APPELLANTS' BRIEF UNDER 37 C.F.R. §1.192

This is an appeal from a Final Rejection dated April 16, 2004, of Claims 1-21. The Appellants submit this Brief in triplicate as required by 37 C.F.R. §1.192(a), with the statutory fee of \$ 330.00 as set forth in 37 C.F.R. §1.17(c), and hereby authorize the Commissioner to charge any

additional fees connected with this communication (including extensions of time) or credit any overpayment to Deposit Account No. 08-2395.

This Brief contains these items under the following headings, and in the order set forth below in accordance with 37 C.F.R. §1.192(c):

- I. REAL PARTY IN INTEREST
- II. RELATED APPEALS AND INTERFERENCES
- III. STATUS OF CLAIMS
- IV. STATUS OF AMENDMENTS
- V. SUMMARY OF INVENTION
- VI. ISSUES
- VII. GROUPING OF CLAIMS
- VIII. APPELLANTS' ARGUMENTS
- IX. APPENDIX A - CLAIMS

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is the Assignee, Lucent Technologies, Inc.

II. RELATED APPEALS AND INTERFERENCES

No other appeals or interferences will directly affect, be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF THE CLAIMS

Claims 1-21 are pending in this Application.

IV. STATUS OF THE AMENDMENTS

The present Application was filed on July 26, 2000, with three independent claims (1, 8 and 15) and a total of 21 claims. On January 8, 2001, the Appellants submitted two references to the United States Patent and Trademark Office (USPTO) in an Information Disclosure Statement (IDS). One of the references submitted in the IDS was an article by Ari Juels and John Brainard from the 1999 proceedings of Networks and Distributed Security Systems (NDSS) entitled "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks" (hereinafter referred to as "Juels"). On November 3, 2003, the Examiner mailed an Office Action rejecting all 21 of the

pending claims under a 35 U.S.C. 103(a) rejection over Juels in view of U.S. Patent No. 6,236,972 to Shkedy (hereinafter referred to as “Shkedy”).

In reply, the Appellants filed an Amendment on January 29, 2004, that corrected an error in the specification and argued against the Examiner’s rejection of the claims. The Examiner did not find the Appellants’ arguments persuasive and issued a Final Rejection on April 16, 2004. On June 7, 2004, the Appellants filed an “Applicant Initiated Interview Request Form” to discuss the Examiner’s response to the Appellants’ arguments in the Amendment and the Examiner’s response to the arguments. More specifically, the Appellants wanted to further discuss that the cited references Juels and Shkedy were not combinable. The interview was conducted on June 15, 2004. On June 16, 2004, the Appellants filed a Notice of Appeal that was received by the USPTO on June 21, 2004.

Subsequently, the Examiner mailed an Interview Summary on June 25, 2004, having a description of the general nature of the interview. The Examiner noted that even though Juels possibly teaches away from utilizing a database, further analysis of Juels would be made. The Examiner also indicated that validating information within a database is extremely well known. The Appellants then filed a “Statement of the Substance of Applicant Initiated Interview In Accordance with C.F.R. §1.133(b)” on July 23, 2004.

V. SUMMARY OF THE INVENTION

The present invention is directed, in general, to computer systems and, more specifically, to a system and method for exacting access costs regarding computer system resources. The present invention introduces a protocol that allows a resource, such as a network server, to require a

potential client to undergo some cost before being granted access to the resource. Thus, instead of simply validating information in a database, the present invention advantageously employs a database of precalculated problems and solutions, such that the resource is not unduly occupied generating problems and solutions for such potential clients. As a result, protocol efficiency is increased without sacrificing protocol integrity.

In one embodiment, the system includes: (1) a database of problems and corresponding precalculated solutions, (2) a problem retriever that responds to a request from a client for access to the resource by retrieving one of the problems from the database and transmitting the one of the problems to the client and (3) a solution evaluator that, upon receiving a putative solution from the client, employs the database to validate the putative solution and, if the putative solution is valid, grants the client access to the resource. A block diagram of an embodiment of a system for controlling access to a resource of a computer system is illustrated in Figure 4 of the present Application (set forth herein as Illustration 1).

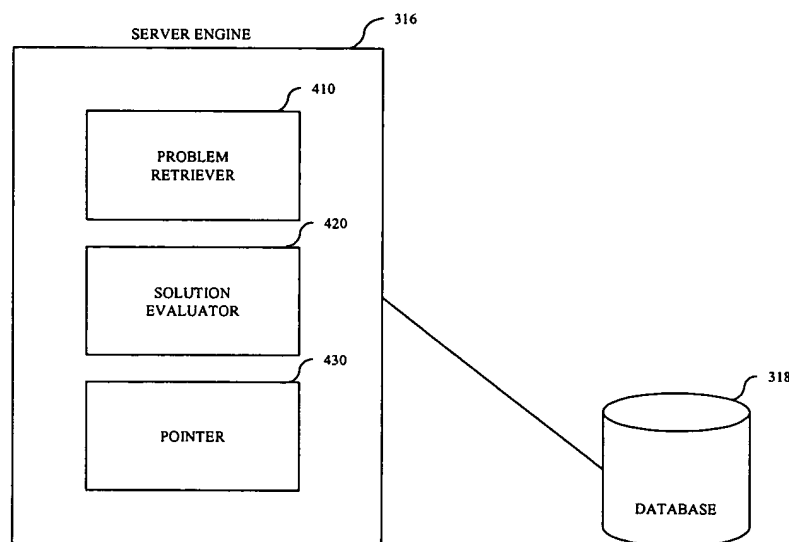


ILLUSTRATION 1

Portions of the system set forth in Illustration 1, a problem retriever 410, a solution evaluator 420 and a pointer 430, are embodied in a server engine 316 and associated with a database 318. Both the server engine 316 and the database 318 are included in a server as illustrated in Figure 3 of the present Application. The database 318 includes problems and corresponding precalculated solutions used in controlling access to a resource of the server. In one embodiment, the problems comprise outputs and portions of corresponding inputs to a one-way function.

Prior to the present invention, when a client computer system or any other computer system wanted to access a resource of a server on a network, such as a web page, the client computer system first established a connection with the server. In establishing a connection, the server allocated stack space for the client and sent an acknowledgment to the client. The client then sent the appropriate requests to access the desired resource. If the client, however, did not respond after receiving the acknowledgment, the client's allocated stack space was kept for a period of time on the server. This delay in deallocating stack space is the basis for connection depletion attacks.

In connection depletion attacks, an attacking system or user will try to make a large number of connection requests to a server in a short period of time. For each connection request, the server allocates stack space to process future requests associated with that particular connection. After the connection is established, the attacking system does not send any further requests on that connection. This causes the server to leave stack space allocated for the established connection. Eventually, the server depletes its available stack space and the server is unable to process new requests.

In one embodiment of the present invention, the present invention combats connection depletion attacks by sending a problem to the client that requests access to a resource. The client

must first solve the problem and send back a putative solution to the problem. The present invention verifies the putative solution before granting the client access to the desired resource.

In the illustrated embodiment of the present invention, the present invention uses the database 318, the problem retriever 410, the solution evaluator 420 and the pointer 430 to combat connection depletion attacks. As described above, the database 318 contains problems and corresponding precalculated solutions. The pointer 430 points to a particular problem/solution entry in the database 318.

When a client requests access to a resource, the problem retriever 410 responds to the request by retrieving a problem from the database 318 according to the pointer 430. The pointer 430 can contain an entry number or a relational index. In another embodiment of the present invention, the problem retriever 410 can use any method to access and retrieve problems from the database 318 with or without a pointer. The problem retriever 410 transmits the problem to the client to solve without allocating any system resources, such as stack space. In another embodiment, the problem retriever 410 transmits the problem and the pointer 430 to the client. The problem retriever 410 then increments the pointer 430. If the pointer 430 exceeds the number of entries in the database 318, the pointer 430 wraps to the beginning entry of the database 318.

The client then solves the problem. For example, if the problem is a MD5 function, the client may be given 120 bits of a 160 bit input and all of the output. The client has to compute the remaining 40 bits of input that when combined with the 120 bits will generate the output. The client incurs computation time (or cost) in order to compute the solution. The amount of input bits to compute and the type of function used can be dynamically adjusted to produce the desired amount of computation time incurred by the client.

Once the client has solved the problem, the client sends the putative solution back to the solution evaluator 420. In another embodiment, the client sends the putative solution and the associated pointer back to the solution evaluator 420. The solution evaluator 420 employs the database 318 to validate the putative solution using the precalculated solution that corresponds to the problem sent to the client. If the putative solution is valid, the solution evaluator 420 grants the client access to the desired resource. In one embodiment, the resource is a network server, an electronic mail server or a main database. In another embodiment, the solution evaluator 420 will establish a connection and allocate stack space or memory upon receiving a valid solution. The server will then process the client's future requests associated with that particular connection.

In the illustrated embodiment, the solution evaluator 420 uses the returned pointer in validating the putative solution. The pointer allows the solution evaluator 420 to index into or relationally access the database 318 without having to maintain a list of problems per request or search the database 318 for the problem and the corresponding precalculated solution. By sending and receiving the pointer 430 that is associated with the problem sent to the client, the problem retriever 410 and the solution evaluator 420 can run stateless. The problem retriever 410 and the solution evaluator 420 do not have to maintain information to associate which problems were sent to which clients. Also, the server does not or is not required to incur more computation time than the client in validating the client's putative solution. Once the solution evaluator 420 receives a valid putative solution, the problem retriever 410 replaces that problem and the corresponding precalculated solution.

VI. ISSUES

Whether Claims 1-21, as rejected by the Examiner, are obvious in accordance with 35 U.S.C. §103(a) over Juels in view of Shkedy.

VII. GROUPING OF THE CLAIMS

Claims 1-21 do not stand or fall together. Independent Claims 1, 8 and 15 form a first group. The dependent Claims form the following groups: Claims 2, 9 and 16 form a second group, Claims 3, 10 and 17 form a third group, Claims 4, 11 and 18 form a fourth group, and Claims 5, 12 and 19 form a fifth group, Claims 6, 13 and 20 form a sixth group and Claims 7, 14 and 21 form a seventh group.

VIII. THE APPELLANTS' ARGUMENTS

The inventions set forth in independent Claims 1, 8, and 15 and each of their respective dependent claims are not obvious over the references relied on by the Examiner.

A. Rejection of Claims 1, 8 and 15 under 35 U.S.C. §103(a)

The Examiner has rejected Claims 1, 8 and 15, which, as set forth above, stand together, under 35 U.S.C. §103(a) as being obvious over Juels in view of Shkedy.

Juels is directed to a cryptographically based countermeasure against connection depletion attacks. When a server comes under attack, it distributes small cryptographic puzzles to clients making service requests. To complete a request, a client must solve its puzzle correctly. (Abstract).

The Examiner asserts that Juels teaches each element of independent Claims 1, 8 and 15 except employing a database to validate a putative solution. (Final Rejection, pages 3 and 5). The Appellants agree that Juels does not teach employing a database to validate a putative solution and also assert that Juels does not suggest employing a database to validate a putative solution since Juels explicitly teaches computing a solution to verify a puzzle instead of using a database. (Page 156, paragraph that starts in column 1 and ends at line 9 of column 2, and Figure 3). Juels, therefore, does not teach or suggest a solution evaluator that, upon receiving a putative solution from a client, employs a database to validate the putative solution and, if the putative solution is valid, grants the client access to a computer system resource as recited in Claims 1, 8 and 15.

Additionally, Juels does not teach or suggest a database of problems and corresponding precalculated solutions as recited in Claims 1, 8 and 15. On the contrary, Juels computes solutions to puzzles so that a “server need not store any puzzle information itself.” (Page 156, lines 2-3 of the second column). Juels, therefore, does not teach or suggest a database of problems and corresponding precalculated solutions or a solution evaluator that, upon receiving a putative solution from a client, employs the database to validate the putative solution and, if the putative solution is valid, grants the client access to the resource.

To teach employing a database to validate a putative solution, the Examiner cites Shkedy. Shkedy, however, also does not teach or suggest a database of problems and corresponding precalculated solutions or a solution evaluator that, upon receiving a putative solution from a client, employs the database to validate the putative solution and, if the putative solution is valid, grants the client access to the resource. In fact, the Appellants do not find any teaching or suggestion in Shkedy of controlling access to resources of a computer system. On the contrary, Shkedy is directed to a

method and an apparatus for facilitating transactions on a commercial network system and is specifically directed to a method and system for facilitating secondary trading of shares of an investment company such as an open-ended mutual fund or a hedge fund. (Column 1, lines 13-17).

Shkedy teaches a cryptographic key database that contains algorithms and keys for encrypting, decrypting and/or authenticating messages. (Column 17, lines 41-43). The keys, however, are not problems and corresponding precalculated solutions as recited in independent Claims 1, 8 and 15. Instead, the cryptographic keys enhance the ability to authenticate a sender of a message and verify the integrity of the message itself, proving that it has not been altered during transmission. Encryption can also prevent eavesdroppers from learning the contents of the message. (Column 17, lines 6-16). Thus, the keys are tools for encrypting and decrypting instead of problems and corresponding precalculated solutions.

Additionally, Shkedy does not teach a solution evaluator that, upon receiving a putative solution from a client, employs the database to validate the putative solution and, if the putative solution is valid, grants the client access to the resource. Instead, the keys are used to encrypt and then decrypt messages, such as orders. For example, a seller encrypts an order with an assigned symmetric key using a cryptographic processor. The encrypted seller order is then transmitted to the cryptographic processor that extracts the seller ID from the seller's bid and looks up the symmetric key of the seller in the cryptographic key database. The seller order is then decrypted with the key. (Column 17, lines 31-41). No putative solution is validated. The cryptographic key database of Shkedy, therefore, is not used to validate a putative solution but to decrypt a customer's message or, alternatively, encrypt the message.

Shkedy, therefore, does not teach or suggest a database of problems and corresponding precalculated solutions or a solution evaluator that, upon receiving a putative solution from a client, employs the database to validate the putative solution and, if the putative solution is valid, grants the client access to the resource as recited in Claims 1, 8 and 15. Accordingly, the cited combination of Juels and Shkedy does not teach or suggest each and every element of independent Claims 1, 8 and 15. Thus, Claims 1, 8 and 15 are not obvious in view of the cited combination.

Furthermore, **even if** Shkedy did teach employing a database to validate a putative solution, one skilled in the art would not be motivated to modify the teachings of Juels with the teachings of Shkedy since Juels explicitly teaches away from employing a database to validate a solution. For example, Juels teaches a client puzzle protocol that requires a puzzle be constructed in a stateless way. In particular, Juels teaches a server **must** be able to verify without the use of a database that a puzzle solved by a client is legitimate. (Page 156, first column, first full paragraph; emphasis added). Juels, therefore, strongly teaches away from combining with any reference employing a database to validate a putative solution and also strongly teaches away from the present invention. Thus, one skilled in the art would not be motivated to combine Shkedy with Juels to arrive at the present invention since Juels explicitly teaches away from employing a database to validate a solution.

B. Rejection of Claims 2, 9 and 16 under 35 U.S.C. §103(a)

The Examiner has rejected Claims 2, 9 and 16 under 35 U.S.C. §103(a) as being unpatentable over Juels in view of Shkedy. The above argument establishing the nonobviousness of independent Claims 1, 8 and 15 is incorporated herein by reference. Dependent Claims 2, 9 and 16 additionally

require that the problems comprise outputs and portions of corresponding inputs to a one-way function, and thereby introduce patentably distinct elements in addition to the elements recited in Claims 1, 8 and 15, respectively. The cited combination of Juels and Shkedy, however, does not teach or suggest that the problems comprise outputs and portions of corresponding inputs to a one-way function in combination with the base claim limitations. Thus, Juels and Shkedy do not establish a *prima facie* case of obviousness of dependent Claims 2, 9 and 16. Accordingly, Claims 2, 9 and 16 are nonobvious over the cited combination of Juels and Shkedy and the Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the Examiner's Final Rejection of Claims 2, 9 and 16.

C. Rejection of Claims 3, 10 and 17 under 35 U.S.C. §103(a)

The Examiner has rejected Claims 3, 10 and 17 under 35 U.S.C. §103(a) as being unpatentable over Juels in view of Shkedy. Dependent Claims 3, 10 and 17 depend on dependent Claims 2, 9 and 16. The above arguments establishing the nonobviousness of independent Claims 1, 8 and 15 and Claims 2, 9 and 16 which depend thereon are incorporated herein by reference. Dependent Claims 3, 10 and 17 additionally require that the one-way function is a Message Digest-5 function, and thereby introduce patentably distinct elements in addition to the elements recited in Claims 1, 8 and 15, respectively. The cited combination of Juels and Shkedy, however, does not teach or suggest that the one-way function is a Message Digest-5 function in combination with the base claim limitations. Thus, Juels and Shkedy do not establish a *prima facie* case of obviousness of dependent Claims 3, 10 and 17. Accordingly, Claims 3, 10 and 17 are nonobvious over the cited

combination of Juels and Shkedy and the Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the Examiner's Final Rejection of Claims 3, 10 and 17.

D. Rejection of Claims 4, 11, and 18 under 35 U.S.C. §103(a)

The Examiner has rejected Claims 4, 11 and 18 under 35 U.S.C. §103(a) as being unpatentable over Juels in view of Shkedy. The above argument establishing the nonobviousness of independent Claims 1, 8 and 15 is incorporated herein by reference. Dependent Claims 4, 11 and 18 additionally require that the problem retriever replaces the one of the problems and a corresponding one of the solutions when the putative solution is valid in addition to the elements recited in Claims 1, 8 and 15, respectively. The cited combination of Juels and Shkedy, however, does not teach or suggest that the problem retriever replaces the one of the problems and a corresponding one of the solutions when the putative solution is valid in combination with the base claim limitations. Thus, Juels and Shkedy do not establish a *prima facie* case of obviousness of dependent Claims 4, 11 and 18, and the Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the Examiner's Final Rejection of Claims 4, 11 and 18.

E. Rejection of Claims 5, 12 and 19 under 35 U.S.C. §103(a)

The Examiner has rejected Claims 5, 12 and 19 under 35 U.S.C. §103(a) as being unpatentable over Juels in view of Shkedy. The above argument establishing the nonobviousness of independent Claims 1, 8 and 15 is incorporated herein by reference. Dependent Claims 5, 12 and 19 additionally require that the problem retriever replaces the one of the problems and a corresponding one of the solutions only when the putative solution is valid in addition to the

elements recited in Claims 1, 8 and 15, respectively. The cited combination of Juels and Shkedy, however, does not teach or suggest that the problem retriever replaces the one of the problems and a corresponding one of the solutions only when the putative solution is valid in combination with the base claim limitations. Thus, Juels and Shkedy do not establish a *prima facie* case of obviousness of dependent Claims 5, 12 and 19, and the Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the Examiner's Final Rejection of Claims 5, 12 and 19.

F. Rejection of Claims 6, 13 and 20 under 35 U.S.C. §103(a)

The Examiner has rejected Claims 6, 13 and 20 under 35 U.S.C. §103(a) as being unpatentable over Juels in view of Shkedy. The above argument establishing the nonobviousness of independent Claims 1, 8 and 15 is incorporated herein by reference. Dependent Claims 6, 13 and 20 additionally require the solution evaluator grants the client access to the resource by allocating memory associated with the resource to serve the client in addition to the elements recited in Claims 1, 8 and 15, respectively. The cited combination of Juels and Shkedy, however, does not teach or suggest that the solution evaluator grants the client access to the resource by allocating memory associated with the resource to serve the client in combination with the base claim limitations. Thus, Juels and Shkedy do not establish a *prima facie* case of obviousness of dependent Claims 6, 13 and 20, and the Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the Examiner's Final Rejection of Claims 6, 13 and 20.

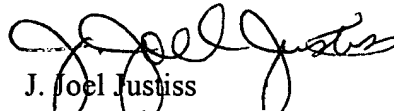
G. Rejection of Claims 7, 14 and 21 under 35 U.S.C. §103(a)

The Examiner has rejected Claims 7, 14 and 21 under 35 U.S.C. §103(a) as being unpatentable over Juels in view of Shkedy. The above argument establishing the nonobviousness of independent Claims 1, 8 and 15 is incorporated herein by reference. Dependent Claims 7, 14 and 21 additionally require the resource is selected from the group consisting of a network server, an electronic mail server and a main database in addition to the elements recited in Claims 1, 8 and 15, respectively. The cited combination of Juels and Shkedy, however, does not teach or suggest that the resource is selected from the group consisting of a network server an electronic mail server, and a main database in combination with the base claim limitations. Thus, Juels and Shkedy do not establish a *prima facie* case of obviousness of dependent Claims 7, 14 and 21, and the Appellants respectfully request that the Board of Patent Appeals and Interferences reverse the Examiner's Final Rejection of Claims 7, 14 and 21.

In summary, the inventions set forth in Claims 1-21 are not obvious in view of the references relied on by the Examiner. The Appellants therefore respectfully request that the Board of Patent Appeals and Interferences reverse the Examiner's Final Rejection of Claims 1-21.

Respectfully submitted,

HITT GAINES, P.C.


J. Joel Justiss
Registration No. 48,984

Dated: 8/5/04

Hitt Gaines, P.C.
P.O. Box 832570
Richardson, Texas 75083-2570
(972) 480-8800
(972) 480-8865 (Fax)
E-Mail: joel.justiss@hittgaines.com

IX. APPENDIX A - CLAIMS

1. A system for controlling access to a resource of a computer system, comprising:
a database of problems and corresponding precalculated solutions;
a problem retriever that responds to a request from a client for access to said resource by retrieving one of said problems from said database and transmitting said one of said problems to said client; and
a solution evaluator that, upon receiving a putative solution from said client, employs said database to validate said putative solution and, if said putative solution is valid, grants said client access to said resource.
2. The system as recited in Claim 1 wherein said problems comprise outputs and portions of corresponding inputs to a one-way function.
3. The system as recited in Claim 2 wherein said one-way function is a Message Digest-5 function.
4. The system as recited in Claim 1 wherein said problem retriever replaces said one of said problems and a corresponding one of said solutions when said putative solution is valid.
5. The system as recited in Claim 1 wherein said problem retriever replaces said one of said problems and a corresponding one of said solutions only when said putative solution is valid.
6. The system as recited in Claim 1 wherein said solution evaluator grants said client access to said resource by allocating memory associated with said resource to serve said client.
7. The system as recited in Claim 1 wherein said resource is selected from the group consisting of:
a network server,

an electronic mail server, and

a main database.

8. A method of controlling access to a resource of a computer system, comprising:
creating a database of problems and corresponding precalculated solutions;
responding to a request from a client for access to said resource by retrieving one of said problems from said database and transmitting said one of said problems to said client;
upon receiving a putative solution from said client, employing said database to validate said putative solution; and
if said putative solution is valid, granting said client access to said resource.

9. The method as recited in Claim 8 wherein said problems comprise outputs and portions of corresponding inputs to a one-way function.

10. The method as recited in Claim 9 wherein said one-way function is a Message Digest-5 function.

11. The method as recited in Claim 8 further comprising replacing said one of said problems and a corresponding one of said solutions when said putative solution is valid.

12. The method as recited in Claim 8 further comprising replacing said one of said problems and a corresponding one of said solutions only when said putative solution is valid.

13. The method as recited in Claim 8 wherein said granting comprises allocating memory associated with said resource to serve said client.

14. The method as recited in Claim 8 wherein said resource is selected from the group consisting of:

a network server,

an electronic mail server, and

a main database.

15. A system for controlling access to a resource of a computer system, comprising:

a database of problems and corresponding precalculated solutions;

a pointer that points to a particular problem/solution entry in said database;

a problem retriever that responds to a request from a client for access to said resource by retrieving one of said problems from said database according to said pointer and transmitting said one of said problems and said pointer to said client; and

a solution evaluator that, upon receiving a putative solution and said pointer from said client, employs said database and said pointer to validate said putative solution and, if said putative solution is valid, grants said client access to said resource.

16. The system as recited in Claim 15 wherein said problems comprise outputs and portions of corresponding inputs to a one-way function.

17. The system as recited in Claim 16 wherein said one-way function is a Message Digest-5 function.

18. The system as recited in Claim 15 wherein said problem retriever replaces said one of said problems and a corresponding one of said solutions when said putative solution is valid.

19. The system as recited in Claim 15 wherein said problem retriever replaces said one of said problems and a corresponding one of said solutions only when said putative solution is valid.

20. The system as recited in Claim 15 wherein said solution evaluator grants said client access to said resource by allocating memory associated with said resource to serve said client.

21. The system as recited in Claim 15 wherein said resource is selected from the group consisting of:

a network server,

an electronic mail server, and

a main database.